RESPONSE TO Notice of Inquiry by the National Institute of Standards and Technology, on the subject of Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace, Billing Code 3510-3, Docket No. 11-524296-1289-02.

Submitter: Dr. Karen Sollins, Massachusetts Institute of Technology, Cambridge, MA 02139
Date: August 25, 2011

Having attended the first two workshops hosted by NIST on the topic of the National Strategy for Trusted Identities in Cyberspace, or NSTIC, I write to raise three primary concerns with respect to the request for comments about governance models. My three concerns are:

1. The lack readiness of the process for a permanent governance structure;
2. A mixing of responsibilities with respect to elements of the Framework approach that would be better served if separated;
3. The proposal that arose from the workshops for a corporation to be formed to take on full responsibility for governance and oversight.

Lack of readiness

I argue that the effort to define a permanent governance structure to undertake the process of the creation of the NSTIC at this time is premature. From listening to presentations, questions, and discussion it is clear that neither NIST nor the community has any clear idea of what is needed, between the level of very high-level abstract statements and very low-level details of bits of candidate technologies to address poorly defined goals. All the space between the statement in the original document and low-level technologies on offer is missing. The realization might range from (1) something as loose as a standards (such as from the IETF), which reflect some agreement among some people on each topic, but only loose consistency and no enforcement, to (2) some middle ground in which practice is vetted for conformance, to (3) a highly organized, rigorously vetted and certified set of capabilities, with both accreditation and enforcement of behaviors. In addition, there was little agreement even about how to interpret the functionality desired from the original document proposing the framework, much less agreement beyond that, in any more detail. Finally there was little or no agreement on the scope of applicability and interoperability, for example whether or not, international cooperation should be a requirement *ab initio* or only after the fact, at some later date.

Recommendation: At this point, I argue that before realizing a permanent governance structure significantly more work is needed to understand the responsibilities and functionality to be expected. Only then can a permanent structure be designed to meet the objectives. Choosing a governance structure without a clear model of its responsibilities seems to be unproductive at best. At present I recommend a small interim group that can make progress on many of the thorny issues, but is not so exclusive as to reduce confidence in the group by the community. This work will require intense work and a commitment to both the process and the timing, because this should not be delayed and lose momentum. The outcome should be a significantly large document that lays out both the expected capabilities and suggested structures (both governance and design) that would lead to a successful effort. In addition, it should have a confidence-inspiring risk analysis. Choosing a permanent governance structure without this preliminary work seems unreasonable to me.

Mixing of kinds of responsibilities

There are several key functions that one can derive from the original Framework proposal. One has to do with overarching architecture, design, and standards adoption (creation where not available,

and acceptance where available). Another has to do with building the components. The proposal is that this part will be left to the private sector and be open to anyone who wants to participate. The third is trust accreditation, tracking of continued compliance with accreditation, and possible enforcement. It is possible that there should be a more refined set of distinctions made as well, but for purposes of this discussion, I will continue with these three. Each requires different knowledge, different skills, and different kinds of responsibilities. There is no reason that any should be undertaken by the organization(s) performing the others. We have standards organizations that have a great deal of experience in understanding the requirements for standards and structures and how to move from one to the other effectively. They are not necessarily the best organizations with the best skills and capabilities to build and operate the elements of such a framework. Neither of these may be the best organizations to test and examine for trust accreditation, and certainly not for enforcement.

Recommendation: Once the community is at a point where a permanent governance structure can be realized, care should be given to assigning responsibilities to the kinds of organizations that are best suited to each element of the Framework. Good solid skepticism should be applied to any suggestion that a single organization might be best at more than one of these elements. It should be noted that by distributing the responsibilities one may also be decreasing the probabilities of decisions being made to meet private objectives.

The pitfalls of creating a legal entity to provide governance

I come from the Internet community. We have before us examples of several organizations created to further the Internet, and one in particular to manage the DNS. I speak of The Internet Society or ISOC and the Internet Corporation for Assigned Names and Numbers, also known as ICANN. ISOC's agenda is probably larger than a corporation that would govern and enable the NSTIC. ICANN's agenda is smaller. Both present us with examples of pitfalls, but both find themselves unable to fund themselves without taking advantage of selling the names (resources) that are at the core of the Internet. Because they have found themselves in that awkward position of going out of business if they don't sell what they chose to architect, they are making choices to further their own bottom lines. I raise this is an example of an unexpected side-effect that has the potential to cause organizations to make decisions that further their own continued existence, perhaps at the expense of the societal need that they were believed to be meeting. It is this sort of conflict of interest that concerns me, with the proposal to create a permanent, legal entity. It will be tempted to make decisions and choices to insure its own longevity first, which may or may not be in the best interests of the rest of the community.

Recommendation: The creation of a corporation as the vehicle for realizing the NSTIC should receive much more careful review, even after the review recommended above of an interim group. It is not an idea that should be picked up without significant careful review.